IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CAROLYN JEWEL, ET AL.,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, ET AL.,

Defendants.

No. C 08-04373 JSW

VIRGINIA SHUBERT, ET AL.,

Plaintiffs,

v.

BARACK OBAMA, ET AL.,

Defendants.

No. C 07-00693 JSW

ORDER DENYING PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT AND GRANTING DEFENDANTS' MOTION FOR PARTIAL SUMMARY JUDGMENT

Now before the Court is the motion filed by Plaintiffs Carolyn Jewel, Erik Knutzen, and Joice Walton, on behalf of themselves and all other individuals similarly situated ("Plaintiffs") for partial summary judgment on their claim for relief which challenges the interception of their Internet communications as a violation of the Fourth Amendment ("Fourth Amendment Claim" or "Claim"). Also before the Court is the cross-motion for partial summary judgment on Plaintiffs' Fourth Amendment Claim filed by Defendants National Security Agency, United States Department of Justice, Barack H. Obama, Michael S. Rogers, Eric H. Holder, Jr., and James R. Clapper, Jr. (in their official capacities) (collectively, "Government Defendants").

Having considered the parties' papers, including the Government Defendants' classified brief and classified declarations, and the parties' arguments, the Court DENIES Plaintiffs'

motion for partial summary judgment and GRANTS the Government Defendants' cross-motion for partial summary judgment.[1]

The issues raised by the pending motions and additional briefing now before the Court compel the Court to examine serious issues, namely national security and the preservation of the rights and liberties guaranteed by the United States Constitution. The Court finds the predicament delicate and the resolution must strike a balance of those significant competing interests.

Based on the public record, the Court finds that the Plaintiffs have failed to establish a sufficient factual basis to find they have standing to sue under the Fourth Amendment regarding the possible interception of their Internet communications. Further, having reviewed the Government Defendants' classified submissions, the Court finds that the Claim must be dismissed because even if Plaintiffs could establish standing, a potential Fourth Amendment Claim would have to be dismissed on the basis that any possible defenses would require impermissible disclosure of state secret information.

BACKGROUND

Plaintiffs allege that as part of a system of mass surveillance, the Government Defendants receive copies of their Internet communications, then filter the universe of collected communications in an attempt to remove wholly domestic communications, and then search the remaining communications for search terms called "selectors" for potentially terrorist-related foreign intelligence information.

The Government has described the collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("Section 702") in several public reports. Upon approval by the Foreign Intelligence Surveillance Court of a certification under Section 702, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, foreign intelligence information designated in the certification. (*See, e.g.*, NSA Civil Liberties and Privacy Office

[1] Having not relied on Plaintiffs' proposed order submitted after the hearing on the motions, the Court DENIES Defendants' motion to strike it.

Report, NSA's Implementation of FISA Section 702 at 4 (Apr. 16, 2014) ("Civil Liberties Report")). Once designated by the NSA as a target, the NSA tries to identify a specific means by which the target communicates, such as an e-mail address or telephone number. That identifier is referred to a "selector." Selectors are only specific communications accounts, addresses, or identifiers. (*See id*; *see also* Privacy and Civil Liberties Oversight Board Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("PCLOB Report") at 32-33, 36.) According to the Government's admissions, an electronic communications service provider may then be compelled to provide the Government with all information necessary to acquire communications associated with the selector, a process called "tasking." (*Id.* at 32-33; *see also* Civil Liberties Report at 4-5.)

One process by which the NSA obtains information related to the tasked selectors is known as the Upstream collection program. Through a Section 702 directive, this program compels the assistance of the providers that control the telecommunications backbone within the United States. (*See* PCLOB Report at 35.) Under the Upstream collection program, tasked selectors are sent to domestic electronic communications service providers to acquire communications that transit the Internet backbone. (*See id.* at 36-37.) Internet communications are filtered in an effort to remove all purely domestic communications, and are then scanned to capture only those communications containing the designated tasked selectors. (*Id.* at 37.) "Unless [communications] pass both these screens, they are not ingested into governmental databases." (*Id.*)

Plaintiffs contend that the copying and searching of their private Internet communications is conducted without a warrant or any individualized suspicion and, accordingly, violates the Fourth Amendment. The Fourth Amendment prohibits the Government from intercepting, copying, or searching through communications without a warrant issued by a neutral and detached magistrate, upon probable cause, particularly describing the place to be searched and the things to be seized. Judicial warrants based on particularity and probable cause are especially crucial in electronic surveillance, where searches

and seizures occur without leaving a trace and where the threat to privacy is especially great. *United States v. U.S. District Court (Keith)*, 407 U.S. 297, 313 (1972).

In their motion for partial summary judgment, Plaintiffs seek adjudication as to their Fourth Amendment Claim with regard only to the NSA's acknowledged Upstream collection of communications pursuant to Section 702. The Government Defendants contend that Plaintiffs' evidence is insufficient to establish standing, and that even assuming standing, either there can be no Fourth Amendment violation on the facts in the record as a matter of law, or alternatively, that the state secrets privilege requires dismissal of Plaintiffs' Fourth Amendment Internet surveillance claim.

The Court shall address other additional specific facts as necessary in the remainder of this Order.

ANALYSIS

A. Summary Judgment Standard.

Summary judgment is appropriate when the record demonstrates "that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). An issue is "genuine" if there is sufficient evidence for a reasonable fact finder to find for the non-moving party. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248-49 (1986). "[A]t the summary judgment stage the judge's function is not . . . to weigh the evidence and determine the truth of the matter but to determine whether there is a genuine issue for trial." *Id.* at 249. A fact is "material" if it may affect the outcome of the case. *Id.* at 248. The party moving for summary judgment bears the initial responsibility of identifying those portions of the record which demonstrate the absence of a genuine issue of a material fact. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986).

Once the moving party meets this initial burden, the non-moving party "may not rest upon the mere allegations or denials of the adverse party's pleading, but the adverse party's response, by affidavits or as otherwise provided in this rule, must set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e). In the absence of such

facts, "the moving party is entitled to a judgment as a matter of law." *Celotex*, 477 U.S. at 323; *see also Keenan*, 91 F.3d at 1279.

B. Standing.

Defendants contend that Plaintiffs have not submitted evidence sufficient to establish that they have standing to challenge the alleged ongoing collection of communications by the NSA. As Defendants admit, the Government has acknowledged the existence of the Upstream collection process which involves the collection of certain communications as they transit the Internet backbone network of telecommunications service providers. However, the technical details of the collections process remain classified.

In order to prevail on their motion for summary judgment, Plaintiffs must support each element of their claim, including standing, "with the manner and degree of evidence required at the successive stages of the litigation." *Bras v. Cal. Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Plaintiffs must proffer admissible evidence establishing both their standing as well as the merits of their claims. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) (holding that the court's ruling on summary judgment must be based only on admissible evidence). If Plaintiffs are unable to make a showing sufficient to establish an essential element of their claim on which they bear the burden at trial, summary judgment must be granted against them. *See Celotex Corp.*, 477 U.S. at 322.

"To establish Article III Standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amnesty International USA*, --- U.S. --- , 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139 (2010)). "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes – that the injury is *certainly* impending." *Id.* (citing *Lujan*, 504 U.S. at 565 n.2) (emphasis in original). Thus, the Supreme Court has "repeatedly reiterated that 'the threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not

sufficient." *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis in original)).

In *Clapper*, the Court found that allegations that plaintiffs' communications were intercepted were too speculative, attenuated, and indirect to establish injury in fact that was fairly traceable to the governmental surveillance activities. *Id.* at 1147-50. The *Clapper* Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to establish a "certainly impending" injury. *Id.*

Here, Plaintiffs have sufficiently demonstrated that they are AT&T customers. (*See* Declaration of Carolyn Jewel at ¶¶ 2-5; Declaration of Erik Knutzen at ¶¶ 2-6; Declaration of Joice Walton at ¶¶ 2-6.) In addition, Plaintiffs allege that, as AT&T customers, all of their Internet communications have been collected and amassed in storage. *See Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974, 991-92 (N.D. Cal. 2006) ("AT&T and the government have for all practical purposes already disclosed that AT&T assists the government in monitoring communication content."). The record suggests that AT&T currently aids the Government in the collection of information transported over the Internet. (*See* AT&T Transparency Report dated 2014.) If the governmental program is sufficiently large and encompassing to include the mass collection of all Internet communications, the question of whether any specific communication was specifically targeted is not the relevant inquiry. *See Klayman v. Clapper*, 957 F. Supp. 2d 1, 26-28 (D.D.C. 2013) (granting standing to individual plaintiffs to challenge NSA collection of their telephone records from Verizon after finding "strong evidence" that NSA collected Verizon metadata for the last seven years and ran queries that necessarily analyzed that data); *see also Smith v. Obama*, 24 F. Supp. 3d 1005, 1007 n.2 (D. Idaho 2014) (finding that plaintiff, a Verizon customer, had standing to bring an action based on collection of telephone metadata). "As FISC Judge Eagan noted, the collection of virtually all telephony metadata is 'necessary' to permit the NSA, not the FBI, to do the algorithmic data analysis that allow the NSA to determine 'connections between known and unknown international terrorist operatives.'" *ACLU v. Clapper*, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013) (citing *In re*

Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], amended clip op. at 22-23); *see also id.* at 748 ("[A]ggregated telephony metadata is relevant because it allows the querying technique to be comprehensive. . . . Armed with all the metadata, NSA can draw connections it might otherwise never be able to find.").

The creation of a large surveillance program designed to "intercept all or substantially all of its customers' communications, . . . necessarily inflicts a concrete injury that affects each customer in a distinct way, depending on the content of that customer's communications and the time that customer spends using AT&T services." *Hepting*, 439 F. Supp. 2d at 1001. In this matter, the Ninth Circuit has held that although the harm alleged by Plaintiffs is widely shared, that does not necessarily render it a generalized grievance. *See Jewel v. Nat'l Sec. Agency*, 783 F.3d 902, 909-10 (9th Cir. 2011) ("[W]e conclude that Jewel alleged a sufficiently concrete and particularized injury, Jewel's allegations are highly specific and lay out concrete harms arising from the warrantless searches."). Accordingly, the Court finds that, as Plaintiffs have provided evidence that they are AT&T customers who send Internet communications, they have crossed the threshold requirement to establish that, should the program work as alleged, their communications would be captured in a dragnet Internet collection program.

However, the question whether Plaintiffs can establish standing to pursue their Fourth Amendment claim against the Government Defendants for constitutional violations goes beyond whether they, as individuals and AT&T customers with Internet communications, can proffer evidence of generalized surveillance of Internet communications. Although the public and admissible evidence presented establishes that Plaintiffs are indeed AT&T customers with Internet communications and would fall into the class of individuals surveilled, the evidence at summary judgment is insufficient to establish that the Upstream collection process operates in the manner in which Plaintiffs allege it does.

In their attempt to establish the factual foundation for their standing to sue on their Fourth Amendment Claim, Plaintiffs rely in large part on the declarations of Mark Klein and their proffered expert, J. Scott Marcus, as well as other former AT&T and NSA employees to

present the relevant operational details of the surveillance program. Plaintiffs assert that the declarations support the contention that all AT&T customers' Internet communications are currently the subject of a dragnet seizure and search program, controlled by or at the direction of the Government. However, having reviewed the record in its entirety, the Court finds the Plaintiffs' evidence does not support this claim.

Plaintiffs principally rely on the declaration of Klein, a former AT&T technician who executed a declaration in 2006 about his knowledge and perceptions about the creation of a secure room at the AT&T facility at Folsom Street in San Francisco. However, the Court finds that Klein cannot establish the content, function, or purpose of the secure room at the AT&T site based on his own independent knowledge. *See* Fed. R. Civ. P. 56(c)(4). The limited knowledge that Klein does possess firsthand does not support Plaintiffs' contention about the actual operation of the Upstream data collection process. Klein can only speculate about what data were actually processed and by whom in the secure room and how and for what purpose, as he was never involved in its operation. In addition, Plaintiffs' expert, Marcus, relies exclusively on the observations and assumptions by Klein to formulate his expert opinion. Accordingly, his testimony about the purpose and function of the secure equipment at AT&T and assumed operational details of the program is not probative as it not based on sufficient facts or data. *See* Fed. R. Evid. 702(b). The Court finds that Plaintiffs have failed to proffer sufficient admissible evidence to support standing on their claim for a Fourth Amendment violation of interference with their Internet communications. In addition, without disclosing any of the classified content of the Government Defendants' submissions, the Court can confirm that the Plaintiffs' version of the significant operational details of the Upstream collection process is substantially inaccurate.

In addition, having reviewed the classified portion of the record, the Court concludes that even if the public evidence proffered by Plaintiffs were sufficiently probative on the question of standing, adjudication of the standing issue could not proceed without risking exceptionally grave damage to national security. The details of the Upstream collection process that are subject the Government's assertion of the state secrets privilege are necessary to

address the defenses against Plaintiffs' theory of standing as well as to engage in a full and fair adjudication of Government Defendants' substantive defenses against the Claim. The Court has reviewed the classified brief submitted by the Government and finds that its legal defenses are persuasive, and must remain classified.

Disclosure of this classified information would risk informing adversaries of the specific nature and operational details of the Upstream collection process and the scope of the NSA's participation in the program. Notwithstanding the unauthorized public disclosures made in the recent past and the Government's subsequent releases of previously classified information about certain NSA intelligence gathering activities since 2013, the Court notes that substantial details about the challenged program remain classified. The question of whether Plaintiffs have standing and the substantive issue of whether there are Fourth Amendment violations cannot be litigated without impinging on that heightened security classification. Because a fair and full adjudication of the Government Defendants' defenses would require harmful disclosures of national security information that is protected by the state secrets privilege, the Court must exclude such evidence from the case. *See Mohamed v. Jeppesen DataPlan, Inc.*, 614 F.3d 1070, 1083 (9th Cir. 2010) (holding that "application of the privilege may require dismissal" of a claim if, for example, "the privilege deprives the plaintiff of information needed to set forth a prima facie case, or the defendant of information that would otherwise give the defendant a valid defense to the claim"). Addressing any defenses involves a significant risk of potentially harmful effects any disclosures could have on national security. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998).

The Court is frustrated by the prospect of deciding the current motions without full public disclosure of the Court's analysis and reasoning. However, it is a necessary by-product of the types of concerns raised by this case. Although partially not accessible to the Plaintiffs or the public, the record contains the full materials reviewed by the Court. The Court is persuaded that its decision is correct both legally and factually and furthermore is required by the interests of national security.

CONCLUSION

For the foregoing reasons, the Court DENIES Plaintiffs' motion for partial summary judgment and GRANTS the Government Defendants' cross-motion for partial summary judgment regarding the allegations of Fourth Amendment violations challenging the possible interception of Plaintiffs' Internet communications.

IT IS SO ORDERED.

Dated: February 10, 2015

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE